https://www.financial-planning.com/news/ai-scams-are-getting-harder-to-spot-how-advisors-can-help

AI scams are getting harder to spot. How advisors can help

By Rob Burgess
February 20, 2025, 5:46 p.m. EST

Imagine getting a phone call from what sounds exactly like your grandson, urgently asking for money because he's in trouble.

He might even send a picture of himself at a hospital.

"In reality, it's not him," said Mithilesh Ramaswamy, senior engineer at Microsoft. "It's an AI-generated voice, cloned from his real conversations. Scammers can now use deepfake technology to mimic voices and even create fake videos, making it incredibly difficult to tell real from fake."

As artificial intelligence-enabled technology rapidly advances, so do the tactics of the scammers who utilize it.

Even those who have dedicated their careers to combatting scammers are targeted. John Wilson, senior fellow of threat research at cyber security firm Fortra, said the firm recently had a scammer leave a deepfake voicemail impersonating the CEO.

Michelle Petrowski, founder and CEO of Being in Abundance in Anthem, Arizona, said she has instructed her clients to never answer "yes" when someone calls and asks if it's them.

"Scammers are recording folks' voices saying 'yes' to fraudulently make purchases and other charges that require voice recognition," she said.

Kyle Newell, financial planner and owner of Newell Wealth Managementin Winter Garden, Florida, said he recently spoke with a client who had a scammer mimic his doctor office's number and attempted to get him to pay for "testing" over the phone.

"It's never-ending, and clients definitely are frazzled by the tactics," he said.

Experts said they have been frustrated by the lack of a coordinated response to these quickly evolving threats, but there are practical steps advisors can take to help protect clients.

AI also enabling more convincing phishing and tech support scams

Ramaswamy said these AI-enabled scams "are evolving at a scale and diversity like we have not experienced before." He said AI is also making phishing emails harder to spot.

"In the past, a scam email might have had obvious grammar mistakes, but today's AI-generated messages are nearly perfect, personalized and highly convincing," he said.

Wilson said prior to 2024, in payroll diversion scams — in which a scammer poses as an employee and attempts to socially engineer a human resources department employee into modifying the real employee's direct deposit account — would generally use awkward phrases and were clearly just a copy-and-paste from a template. (For example: "i wish to update my bank information before the next payroll is processed. what details do you need?")

"Recently we've started seeing greater variation in the message content," he said. "Our conclusion is that, yes, scammers are starting to utilize AI."

For example, Wilson said his firm recently saw the following message: "I hope this message meets you well. I'm reaching out to let you know that I've recently changed banks and I would like to request an update to my direct deposit information before the upcoming pay period is finalized."

Leibel Sternbach, founder of retirement planning platform Yields4U.com, said his mother-in-law — a retired CPA, who was running multiple successful nursing homes — fell victim to multiple romance and tech support scams, which involved her sending money, electronics, gift cards and cryptocurrency.

Ramaswamy said a common version of tech support scams comes through pop-up alerts on computers.

"You might be browsing the web when suddenly a warning appears, saying your computer is infected and urging you to call a tech support number," he said. "If you do, the scammer on the other end will pretend to fix the issue while stealing your data and installing malware on your PC."

Centralized reporting and response sorely lacking

During a recent North American Securities Administrators Association (NASAA) webinar, Ken Westbrook, founder and CEO of the nonprofit Stop Scams Alliance,called for a sweeping White House-led, cross-government, cross-industry, public-private partnership response to these international, technology-enabled scams.

"The U.S. needs a national, whole-of-government strategy, with goals, metrics and resources," he said.

Wilson said there actually is a centralized place to report scams, the FBI's Internet Crime Complaint Center (IC3) — but "the cruel joke here is that the people who know about [it] are usually quite savvy about online scams, while the people who are the most susceptible to scams have no idea of where to report them."

Paul Theobald, partner at M&A cyber advisory firm Blackswan Cyber said the IC3 serves a critical role, but "due to limited staffing, many reports don't get immediate, or any, follow-up unless they hit an unofficial 'minimum loss threshold' that's set high."

"I've seen instances where attorneys with strong government ties can secure additional help, but those cases are rare," he said. "More resources for IC3 would improve responsiveness, though given current government hiring trends, that seems unlikely soon."

Sternbach said in his experience, it is almost impossible to report these crimes to the authorities.

"The FBI won't take on the case until there is a local police report," he said. "The local police department oftentimes doesn't want to deal with, or they don't have the resources. Once you get a case open with the local police department, getting the FBI to take interest is difficult."

Calum Baird is a digital forensics and incident response consultant who spent nearly a decade as a detective for Police Scotland, including three years working cybercrime investigations. He said there has been a similar issue in the U.K. with there being multiple police forces and different guidance for reporting cybercrime depending on location.

"A major challenge of cybercrime is that it can be perpetrated from essentially anywhere in the world due to the internet," he said. "This often leads to challenges in investigations and enforcement action as cybercriminals will often operate in, or via, countries that do not typically cooperate with one another. An example of this would be cybercriminals targeting U.S. businesses via servers and technical infrastructure in Russia. In an ideal world, more cooperation between countries in tackling cybercrime would be a step in the right direction. However, with geopolitical tensions and conflicts, this is not likely to happen in the near future."

Ramaswamy said the scammers are possibly in different countries than the victims and are subject to different laws.

"Since crimes need to be investigated and prosecuted on a case-by-case basis, the amount lost, even if it's significant for an individual, is very small compared to the cost of resources which need to be invested to investigate the individual crime," he said.

Having a national registry, education and "parading these cases out in the public" would go a long way to reducing the stigma associated with these crimes, said Sternbach.

"The fact that countries like Russia, North Korea and Iran can fund significant portions of their economy off the backs of our seniors is appalling," he said. "We

can and should make this a national security issue and put an end to it."

Advisors can provide a human connection with vulnerable clients

Even when there are mechanisms to report scams, Sternbach said victims often don't want to, as they either don't feel like they have been scammed or are ashamed. He said one of the first steps that these criminals take when grooming victims is to create a wedge between them and their families.

"They create secret codes and vilify the family members who can spot the behavior or who actively are trying to stop it," he said. "The scammers actively create an environment where the victim feels like their family is taking advantage of them, abusing them and it is only their scammer who is their true friend in the world. The person who 'gets' them and wants what is best for them, means they may never accept that they have been scammed, especially if they are mentally and emotionally compromised, which is often the reason why they are vulnerable to these scammers in the first place."

The sad fact of the matter is that these technology-enabled scams prey on the most vulnerable. In 2023, scams targeting individuals aged 60 and older caused over $3.4 billion in losses — an increase of approximately 11% from the year prior, according to the FBI.

Marcelo Barros, cybersecurity leader at cybersecurity education firm Hacker Rangers, said the elderly are often seen as "easy targets for cybercriminals because they tend to have financial reserves and are more trusting when approached by phone calls or text messages."

Sternbach said since falling victim to these scams, his mother-in-law has now been diagnosed with dementia. However, in hindsight, at the early stages of her disease — before they realized that her judgment was compromised — she became susceptible to these scammers who took advantage.

"After going through this personally, I think the only real way to combat these types of scams is to ensure that you have an advisor or trusted contact on your accounts who will notice you suddenly taking out large portions of your life savings to buy Amazon gift cards, or suddenly spending lots of money on laptops or online purchases," said Sternbach. "It is one of the hidden values that we bring as advisors, is just serving as a protector who can spot the signs of elder abuse and work to mitigate it."

The best defense against scams is knowledge, vigilance and a "healthy dose of skepticism," said Ramaswamy.

"If something feels off, or it sounds too good to be true, it probably is," he said.

Christopher Rand, managing partner and personal chief financial officer at FIDES Wealth Strategies Group and The Wealth Consulting Group in Las Vegas, said he has had several instances of emails where the language, tone and

sentence structure were out of character for the client. When the advisor called the client directly to ask if they had in fact sent the email, it was discovered they had not and were unaware that a scammer had hacked into their email account.

"I believe that the personal relationships advisors have with their clients adds some level of account security as they may notice inconsistencies like that," he said.

Practical steps advisors can take

Ramaswamy said he encouraged advisors to help set up two-factor authentication (2FA) on their accounts, "which acts like a double lock on their digital doors." Even if a scammer gets their password, they won't be able to access the account without the second authentication step, he said.

Theobald said advisors should encourage clients to invest in a dedicated tablet and create an email address strictly for banking activities.

"The tablet doesn't get used for anything, including internet browsing," he said. "The email is only for your bank accounts."

Additionally, a data removal membership generally costs between $100 and $300 and is well worth the expense, said Theobald.

"Your name, address and phone number is collected and sold across hundreds of data brokers," he said. "That is the info that scammers use to target you."

AJ Thompson, chief commercial officer at IT consultancy Northdoor said he recommended implementing regular family awareness sessions, establishing verification protocols for large transfers and requiring voice confirmation for any unusual account activity.

"It's important to remember that these social engineering tricks are always evolving, and awareness training has to be kept fresh and up to date," he said.

Rand said he regularly calls clients back when receiving emails or mail about money movement instructions. He said they have added fraud watches to some clients' accounts with their custodians when they are at a higher risk for scams.

"Financial education only goes so far," he said. "Education related to identifying scams needs better dissemination to the public, especially the vulnerable."